**WILLKIE FARR & GALLAGHER LLP**
Benedict Y. Hur (SBN: 224018)
Simona Agnolucci (SBN: 246943)
Eduardo E. Santacana (SBN: 281668)
Amanda Maya (SBN: 324092)
One Front Street, 34th Floor
San Francisco, CA 94111
Telephone: (415) 858-7400
Facsimile: (415) 858-7599
bhur@willkie.com
sagnolucci@willkie.com
esantacana@willkie.com
amaya@willkie.com

Attorneys for
GOOGLE LLC

**UNITED STATES DISTRICT COURT**

**NORTHERN DISTRICT OF CALIFORNIA**

**SAN FRANCISCO**

ANIBAL RODRIQUEZ *et al*., individually and on behalf of all other similarly situated

Plaintiffs,

vs.

GOOGLE LLC, *et al*.,

Defendant.

Case No. 3:20-CV-04688 RS

**DEFENDANT GOOGLE LLC's REPLY IN SUPPORT OF MOTION TO DISMISS FIRST AMENDED COMPLAINT**

Judge: Hon. Richard Seeborg
Court: Courtroom 3 – 17th Floor
Date: March 4, 2021
Time: 1:30 p.m.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Statutes

## INTRODUCTION

Plaintiffs' First Amended Complaint ("FAC") is premised on trying to connect two unrelated things: the Google Account setting called Web & App Activity ( "WAA") and the Google tool used by app developers called Google Analytics for Firebase ("GA for Firebase"). Plaintiffs claim that when third-party app developers choose to use GA for Firebase to analyze data (instead of another company's tool) that renders unrelated disclosures about the WAA setting misleading. Plaintiffs don't allege that app developers lack the right to analyze Plaintiffs' data, nor that app developers lack the right to use a third-party to do it. Nor do they allege that WAA (which, when on, saves searches and activity on Chrome and *Google* apps and services) stores the same data that users provide to the third-party apps. To the contrary, Google has provided judicially noticeable public sources demonstrating that: (1) app developers knowingly use GA for Firebase to collect app-usage data; (2) app developers are required to (and do) obtain consent for the use of GA for Firebase to analyze that data; and (3) WAA—whether on or off—does not store third-party app usage data from GA for Firebase in a user's Google account, anyway. The opposition tries to distract the Court from the necessary implications of their factual allegations—that app developers intentionally integrated, and users knowingly consented to, GA for Firebase, a traditional analytics tool that tracks and reports statistics about, *e.g.*, which recipes are most popular on a cooking app and which lessons are most popular on a language instruction app.

Plaintiffs argue that the consent app developers provided to Google was conditioned on whether an individual had WAA on or off, but there is nothing in their FAC to support that assertion, and the theory, when taken to its logical conclusion, would be nonsensical. Plaintiffs also assert that they understood WAA was meant to permit a user to shut off all data flow to Google about that user, whether or not they are using a Google product or service, because the use of the word "service" is defined elsewhere to include Google products integrated into third-party apps. That argument ignores the actual language of the disclosure, as well as the rest of the same disclosures Plaintiffs rely on, which repeatedly and comprehensively disclosed the facts Plaintiffs now complain they didn't know. Every claim fails because there was mutual consent.

Perhaps recognizing that the consent to GA for Firebase provided by both app developers

and their users is fatal to every claim, Plaintiffs pivot away from the FAC's allegations. While the FAC complains of the collection and analysis of app user data (GA for Firebase), the opposition argues that the "secret scripts" it complains of are not in GA for Firebase, but rather in some undisclosed portion of Firebase SDK. Such accusation falls woefully short of the Rule 8 pleading standard. Despite making 80 pages of allegations, if Plaintiffs are not accusing GA for Firebase, the FAC fails to put Google on notice of what functionality of Firebase SDK is at issue in this case, and Plaintiffs cannot use their brief to salvage their insufficient pleading.

## ARGUMENT

### I. Plaintiffs' pivot to a "secret scripts" theory is unsupported by factual allegations.

Google's motion to dismiss focuses on GA for Firebase because the FAC's factual allegations—to the extent that they describe anything within Firebase SDK at all—relate to GA for Firebase alone. Plaintiffs' attempts to pivot away from GA for Firebase, and to instead accuse "secret scripts" (which would have to be part of one of the other 18 products that make up Firebase SDK), *see* Opp. at 5–6, are improper and unsupported by their factual allegations.[1] *In re Facebook, Inc. Sec. Litig.*, 477 F. Supp. 3d 980, 1020 (N.D. Cal. 2020) ("It is well established that a complaint may not be amended by briefs in opposition to a motion to dismiss.").

The FAC alleges that Plaintiffs' privacy was violated by Firebase SDK, a "platform" that app developers use to "build their apps."[2] FAC ¶ 3. They further allege that Firebase SDK includes, among other things, the "Google Analytics" for Firebase service. *Id.* ¶ 42(a).

The universe of factual allegations concerning accused functionality consists of just fifteen paragraphs targeting GA for Firebase as the offending product: paragraphs 42 and 44–58 of the FAC. Those paragraphs allege that "software scripts . . . cause the apps to copy and transmit to Google's servers . . . many different kinds of user communications between" the users and the

[1] The parties agree that Firebase SDK and GA for Firebase aren't the same thing. As Google explained in its motion, the latter is one product offered as part of the former. *See* Mot. at 2–3; Opp. at 1–2. The parties further agree that not all users of Firebase SDK use GA for Firebase, which is optional. *See* Mot. at 2–3; Opp. at 7–8 (conceding app developers consented to at least "some" of GA for Firebase voluntarily).

[2] Quotation marks and alterations have been omitted and emphases added, unless stated otherwise.

apps. FAC ¶ 44. The "Google Analytics service" is meant "to gain information about customers' use of the app." *Id.* ¶ 42(a). The footnotes in these paragraphs provide the basis for Plaintiffs' allegations: public documentation published by Google explaining how "Google Analytics-Android" and "Google Analytics-iOS," *i.e.*, GA for Firebase, works. Those sources include:

- developer portal documentation for GA for Firebase (*see* footnote 11);
- documentation about GA for Firebase concerning "automatically collected events" (*see* footnotes 14 and 16, which link to a page explaining that "Analytics collects events for Android and iOS apps unless otherwise stated."); and
- documentation about GA for Firebase concerning properties tags (*see* footnote 15).

These paragraphs and footnotes explain that GA for Firebase compiles statistics about the popularity of app content and that the GA for Firebase scripts allow developers to log and send to Google "the user's interactions with the app, including viewing content, creating new content, or sharing content. *Id.* ¶¶ 49–50. And they explain that GA for Firebase operates by logging "events" and "parameters" as described in the help center pages they cite. *Id.* ¶¶ 51–55. None of this is controversial. Analytics tools are an integral part of how the Internet works.[3]

Thus, while Plaintiffs assert in their opposition that the FAC is *not* about GA for Firebase, the only *facts* pleaded in the FAC relate to GA for Firebase.[4]

Plaintiffs argue in footnote 1 of the opposition that the FAC contains allegations about "secret scripts" in Firebase that transmit user data to Google *whether or not Google Analytics is turned on*. But an exhaustive search for that allegation in the FAC itself turns up nothing. The

[3] *See, e.g.*, https://en.wikipedia.org/wiki/Web_analytics.

[4] There is a lone footnote in the FAC— no. 13—that links to a webpage unrelated to GA for Firebase; it links to the "App Indexing" product offered as part of Firebase SDK. *See* Supp. Req. for Jud. Not., Ex. A (https://firebase.google.com/docs/app-indexing/android/log-actions). Plaintiffs seem to have cited that webpage by mistake. The page makes plain that App Indexing is a different product that includes logging user actions for app developers. But as the Court can see for itself, in a big purple box on the same webpage, Google instructs developers that no personal information should go to Google servers and that users must provide consent for App Indexing on their myactivity.google.com page (*i.e.*, WAA). No other allegations pertain to or even mention App Indexing. And the specific allegation for which the App Indexing page is cited contains no allegations that could give rise to liability. This footnote citation standing alone cannot support an entire claim without further factual enhancement.

cited paragraphs, FAC ¶¶ 45, 117–20, say no such thing. Similarly, the opposition claims that the collection of the types of data identified in the FAC as offending "occurs *whether or not an app developer has enabled Google Analytics*." Opp. at 6:8–10. Plaintiffs provide no cite there because there isn't one; there is no such allegation in the FAC, and if there were, it would be false.

Where a complaint makes a "naked assertion of conspiracy" without "further factual enhancement," that "stops short" of the plausibility standard. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 557 (2007). Similarly, "bare assertions . . . are not entitled to the assumption of truth" unless there are alleged "facts that nudge[ the] claims . . . across the line from conceivable to plausible." *Ashcroft v. Iqbal*, 556 U.S. 662, 680 (2009). The "secret scripts" allegations here are indistinguishable from the conspiracy theories in *Twombly* and *Iqbal*. There are no *facts* alleged that support Plaintiffs' bare assertions that Firebase SDK contains offending secret scripts. And the only facts that are alleged are comprehensively cited to *public* documentation published by Google for Firebase customers who use GA for Firebase. Indeed, to believe the opposition's "secret scripts" theory is to believe that Google created two analytics systems—GA for Firebase, which is publicly and extensively documented, and a shadow copy of GA for Firebase that does the same thing but is not disclosed to app developers or users. There isn't a single fact alleged in the FAC that would render such a claim plausible. It deserves no credence.[5]

Plaintiffs' "secret scripts" theory suffers from another problem: it sounds in fraud. Plaintiffs' claim that Google surreptitiously embedded secret code to take user data against user's contrary expressed wishes triggers the heightened pleading standard that applies to claims supported by allegations of fraud (even if the claim itself is not a fraud claim), and these allegations fall far short of the familiar Rule 9(b) standard. *See, e.g.*, *Vess v. Ciba-Geigy Corp. USA*, 317 F.3d 1097, 1103–04 (9th Cir. 2003) (even where claim is not one of fraud, if plaintiff alleges a "course of fraudulent conduct" and relies on that course of conduct "as the basis of a claim," the claim is "grounded in fraud" and its pleading "must satisfy the particularity

[5] In any event, while Firebase SDK is made up of 19 different products, whichever ones Plaintiffs may later accuse, Google will be able to cite disclosures demonstrating that the app developers and their users consented to Google receiving and processing any of the app users' data.

requirement of Rule 9(b).”). Further, Plaintiffs’ “secret scripts” allegations are entirely made on information and belief, and much more than that is required to pass muster. *See, e.g.*, *McFarland v. Memorex Corp.*, 493 F. Supp. 631, 639 (N.D. Cal. 1980) (a plaintiff pleading on information and belief must provide “sufficient detail to demonstrate that his complaint is grounded in some facts.”); *Pirelli Armstrong Tire Corp. Retiree Med. Benefits Tr. v. Walgreen Co.*, 631 F.3d 436, 442 (7th Cir. 2011) (“A plaintiff who alleges fraud can provide all the detail in the world, but does not have unlimited leeway to do so on ‘information and belief.’”).

## II. Plaintiffs fail to state a claim under the Wiretap Act.

Plaintiffs concede that consent by either party to a communication is fatal to a federal Wiretap Act claim. *See In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1026 (N.D. Cal. 2014) (quoting 18 U.S.C. § 2511(2)(d)). Their opposition fails to grapple with this fatal defect.

### A. App developers chose to use GA for Firebase and explicitly consented to it.

Plaintiffs concede that app developers who choose to use GA for Firebase consent to its use. And they concede that the GA for Firebase Terms of Use (“ToU”) require app developers to obtain users’ consent and forbid them from sending personally identifiable information (PII) about their users to Google. Mot. at 3–6. Plaintiffs also concede that GA for Firebase is an optional component of Firebase SDK. Indeed, Plaintiffs’ opposition turns on unsupported speculation about what happens in a Firebase SDK app when the app developer *disables* GA for Firebase. Nor do Plaintiffs dispute that for the apps they identified, app developers in fact complied with Google’s contractual terms requiring that they obtain user consent and avoid sending PII. *Id.*[6]

Instead of disputing these points, Plaintiffs argue that app developers’ consent depended on the consent of their users; per Plaintiffs, Google failed to disclose in the ToU that GA for Firebase would work the same way whether or not a user had turned the WAA setting to off. Opp. at 4:15–24. Plaintiffs’ speculation about the expectations of third-party app developers—who are not their

[6] Even though Plaintiffs argue there must be other unidentified apps that use Firebase SDK, there’s no allegation that any such app failed to obtain the user consent they were required to obtain, either. Even if Plaintiffs could identify such an instance, there are no allegations that would support a finding of liability against Google for that; Google’s terms unambiguously require app developers to obtain consent.

clients—is a bald assertion. Nothing in the ToU suggests that data collection will depend on a user's WAA setting, and nothing anywhere else suggests that app developers expected it to. Indeed, it would defy common sense for app developers to knowingly give up the right to analyze activity on the app by virtue of using GA for Firebase as opposed to a different analytics tool.

Regardless, Plaintiffs' argument is legally unsupportable. Plaintiffs have cited nothing to support that view, and Google is unaware of authority that an end user can grant or revoke an app developer's consent to the transmission of their communication to Google. While consent may not be an "all-or-nothing proposition," it certainly isn't an "only if someone else consents" proposition, either.[7]

**B. The Users Consented to GA for Firebase.**

Plaintiffs emphasize their commitment to their personal privacy. It is fair, then, to hold them to the policies and disclosures they rely on for their claims. Those policies and disclosures couldn't be clearer: Google acts as a data processor for GA for Firebase customers, and if an end user of a third-party app wants to opt out of GA for Firebase, that's between the user and the app developer. Plaintiffs consented to each app's terms of use, and their toggling of WAA did not alter, amend, or revoke that consent.

**1. Plaintiffs consented to the use of GA for Firebase.**

The GA for Firebase Terms of Service agreement requires app developers to "disclose the use of the [GA for Firebase] Service, and how it collects and processes data" and to "ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device." Mot. at 4 (quoting Rope Decl. Exs. 1(a) at 5, 1(b) at 14. The apps at issue did just that. For example, Alibaba's Privacy Policy expressly discloses that its "Platform uses Google Analytics" and that "data generated by the cookie about your use of the Platform will be transmitted to Google." Mot. at 4 (quoting Mitchell Decl. Ex. B(1), B(2); *see also* Mot. at 4–5, 11–12 (describing disclosures made by accused apps).

[7] The opposition doesn't attempt to support the FAC's far-fetched allegations that developers were "coerced" to use Firebase SDK. That app developers must use Firebase SDK in order to access certain other Google services is not coercion under any definition of the word. *See* FAC ¶ 42. And, even if they were coerced to use Firebase SDK, GA for Firebase is nevertheless optional.

Plaintiffs' opposition ignores these disclosures, and argues at least 17 times that Google's Privacy Policy failed to disclose information about GA for Firebase, or that Google somehow breached its Privacy Policy. The opposition also relies on at least five other alleged representations Google made about privacy, as well as the information Google provides about how WAA works.

But the opposition rarely addresses the actual language of the Privacy Policy, and when it does, it presents the language out of context. Google's Privacy Policy discloses the range of information Google may receive about users, how users can control that flow of information, and what Google uses that information for. It explains, that Google may share information with "[t]hird parties to whom you consent to sharing your information, such as services that integrate with Google's services." FAC, Ex. A at 19. And it discloses under the heading "your activity on other sites and apps," that

> [m]any websites and apps partner with Google to improve their content and services. For example, a website might use our advertising services (like AdSense) ***or analytics tools (like Google Analytics)***, or it might embed other content (such as videos from YouTube). ***These services may share information about your activity with Google*** and, depending on your account settings and the products in use (for instance, when a partner uses Google Analytics in conjunction with our advertising services), ***this data may be associated with your personal information***.

FAC Ex. A at 32. Below that, Google provides a link to "[l]earn more about how Google uses data when you use our partners' sites or apps." *Id.* That webpage is also part of the "Privacy & Terms" portal, and is titled "HOW GOOGLE USES INFORMATION FROM SITES OR APPS THAT USE OUR SERVICES."[8] It explains that "when you visit a website that uses . . . Google Analytics . . . your web browser automatically sends certain information to Google" including "your IP address" and "the page you're visiting." Mitchell Decl., Ex. N. And it explains that "Google uses the information shared by sites and apps" for a variety of purposes, including to "personalize content and ads you see on Google and on our partners' sites and apps." *Id.* Finally, that page discloses that "[Google] will respect the purposes described in the consent you give to the site or

[8] https://policies.google.com/technologies/partner-sites. Google did not incorrectly identify Exhibit N as Google's Privacy Policy. The Mitchell Declaration identifies Exhibit N as the Google Privacy & Terms web page, which is part of the same portal that includes the Privacy Policy, and to which the policy links. Mitchell Decl. ¶ 16.

app, ***rather than the legal grounds described in the Google Privacy Policy. If you want to change or withdraw your consent, you should visit the site or app in question to do so***."[9] *Id*.

The Privacy Policy also discloses that "Google Analytics relies on first-party cookies, which means the cookies are *set by the Google Analytics customer*." *Id.* at 27. And to make it perfectly clear, the policy also states that "[t]his Privacy Policy doesn't apply to services that have separate privacy policies that do not incorporate this Privacy Policy." *Id.* at 18.

That page also invites the user to learn yet more about "Google Analytics and privacy." The link leads to a page called "Safeguarding your data," which walks through data security policies for complying with, *inter alia*, the California Consumer Privacy Act. Supp. Req. for Jud. Not., Ex. B at 1-5. It explains that Google operates as a "data processor" for Google Analytics, and as such, it "collects and processes data on behalf of our clients, pursuant to their instructions." *Id.* at 1. And it explains that "[w]here sites or apps have implemented Google Analytics with other Google Advertising products, like Google Ads, additional advertising identifiers may be collected. Users can opt-out of this feature and manage their settings for this cookie using the Ads Settings." *Id.* Finally, under the heading "Data Collected by Google Analytics," it explains that "Google Analytics collects . . . on-site/app activities to measure and report statistics about user interactions on the websites and/or apps that use Google Analytics." *Id.* at 2.

In light of these disclosures, the Court should find as a matter of law that users consented to GA for Firebase. *See, e.g.*, *In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1029 (holding at motion to dismiss that Yahoo terms expressly disclosed challenged practice).

**2. WAA didn't override the many instances of consent Google obtained.**

The opposition misses the forest for the trees. Instead of acknowledging these comprehensive disclosures, they identify two partial phrases they say revoked consent for GA for Firebase and rendered every disclosure above meaningless. They argue that when a user turns off WAA, an account-level setting that does not even store third-party app data saved by GA for

[9] The GA for Firebase Terms of Service notifies app developers that they must notify users that they are using GA for Firebase and identify how this service collects and processes data. Google explained that this could be done by displaying a prominent link to this same webpage, located at www.google.com/policies/privacy/partners/. Rope Decl. ¶ 2.

Firebase, that somehow revokes the express consent users provide to third-party apps to use GA for Firebase. *See* Opp. at 9–12. They say this is so because WAA is described as a service that can, among other things, save data about user "activity on sites, apps, and devices that use Google services." Opp. at 10. And because the Privacy Policy's first page explains that "[o]ur services include . . . [p]roducts that are integrated into third-party apps and sites, like ads and embedded Google Maps," that means WAA reaches GA for Firebase and should turn it off when WAA is turned off. *See* FAC ¶¶ 5, 66–68 & Ex. A at 1, 9; Opp. At 10:12. That's wrong.

***First***, the premise of Plaintiffs' "services" exegesis is unreasonable. WAA can save data in a user's account about "apps . . . that use ***Google services***," which are "[p]roducts that are integrated into third-party apps and sites, like ads and embedded Google Maps." FAC ¶ 5. GA for Firebase is not a "product . . . like ads and embedded Google Maps." It's not an embedded Google service at all. Its purpose is not for Google users to use it, because it isn't even aimed at users. Google services are Search, Ads, Maps, YouTube, etc. Everywhere where the Privacy Policy uses this language, that's made clear. *See, e.g.*, FAC, Ex. A at 2 ("you can use many Google services when you're signed out . . . like searching on Google or watching YouTube videos"). Google explains that it collects information about their users' activity "in our services" which "may include: Terms you search for; Videos you watch," etc. *Id.* at 4. Plaintiffs cannot engage in activity "in" GA for Firebase because it isn't a user service.[10]

Further, after listing examples of what's saved in "My Activity," the policy explains that "[y]ou can visit your Google Account to find and manage activity information that's saved in your account." *Id.* at 4. Anyone who would have visited that page would have known that it saves data about Google user-facing services like Search and Maps, not GA for Firebase.[11]

---

[10] Indeed, the opposition concedes that WAA doesn't store data collected by GA for Firebase in a user's Google Account or "My Activity" page. Mot. at 6:21–26.

[11] The opposition correctly recounts that the GA for Firebase Use Policy says app users can opt out of GA for Firebase "through applicable device settings," but then asserts that WAA is "one such setting" without any support. Opp. at 7:8. The cited paragraphs say the opposite: turning WAA on or off is device-agnostic; WAA is an account setting, not a device setting. The same privacy policy on which Plaintiffs rely so heavily explains the difference between account-level and device-level settings in various ways. *See, e.g.*, FAC, Ex. A at 4 ("The types of location data we collect depend in part on your *device* and *account* settings."), 12 ("Device-level settings: Your

The two phrases relating to "services" cannot hold up Plaintiffs' entire case under the weight of the avalanche of other, express, fulsome disclosures.

***Second***, Plaintiffs overstate the role WAA plays at Google as a form of "user control" by focusing exclusively on it. WAA is one of *many* privacy controls available to Google users. *See* FAC Ex. A at 8–9 (describing almost a dozen different privacy controls). It is not a single valve that can control the entire flow of data on the Internet. The Privacy Policy outlines how these controls work to give users granular control over their privacy. The same policy discloses that GA for Firebase collects user data at the behest of app developers subject to separate policies. And it discloses that users will be bound the separate consent they give app developers.

***Third***, Plaintiffs' argument, taken to its logical conclusion, makes no sense. They claim Google should break how GA for Firebase works for any third-party app users who are also Google account-holders and who turned WAA off. But, paradoxically, since app developers are barred from sending PII to Google, Google would have to try to unmask each user of each app using GA for Firebase every time the user uses it to determine whether that user's WAA setting is on or off. Then, for those users Google can unmask, their usage data would have to be removed from the statistics on page views and other similar pieces of information that app developers would otherwise receive. None of that passes the smell test.

Plaintiffs make the last ditch argument, in a footnote, that consent is a fact issue. Opp. at 6 n.2. They don't flesh out that argument any further, and for good reason. Though it may sometimes require factual development, consent is often apparent from the face of the complaint and judicially noticeable documents. That is the case here, as it has been in many other cases. *See* Mot. at 9, 12–13 (citing cases); *see also In re Yahoo Mail Litig.*, 7 F. Supp. 3d at 1029.

**C. Plaintiffs over-extend the crime-tort exception; it doesn't apply here.**

Plaintiffs also argue that Google can be liable under the Wiretap Act regardless of consent if the interception was done with an unlawful or criminal purpose, *i.e.* the crime-tort exception. Opp. at 13. That argument fails at step one. To qualify under this exception, "the offender must

---

device may have controls that determine what information we collect.").

have as her objective a tortious or criminal result." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). Plaintiffs must allege either the "primary motivation or a determining factor in the interceptor's actions has been to injure plaintiffs tortiously." *In re Google Inc., Gmail Litig.*, No. 13-md-02430-LHK, 2014 WL 1102660, at *18 n.13 (N.D. Cal. Mar. 18, 2014). The exception applies only where the interception is "done for the purpose of facilitating some further impropriety, such as blackmail." *Sussman v. Am. Broad. Cos.,* 186 F.3d 1200, 1202 (9th Cir. 1999).

Plaintiffs argue that Google's alleged criminal or tortious purpose was to compile user data in order to make greater profits from ad targeting.[12] Opp at 13. Even if true, that purpose would fall short of criminal or tortious. Courts across the country are in agreement in very similar postures.[13] Plaintiffs' cases do not compel a different result. *Planned Parenthood Fed'n of Am., Inc. v. Ctr. for Med. Progress*, 214 F. Supp. 3d 808, 828 (N.D. Cal. 2016), involved a large "criminal enterprise," far afield of the allegations here. And *In re: Maxim Integrated Prods., Inc.*, No. 12-244, 2013 WL 12141373, at *15 (W.D. Pa. Mar. 19, 2013), is an out-of-district case that held a different statute than any claim at issue here could serve as a predicate for the crime-tort exception; the decision has never been cited for that proposition, and reading it as permitting a claim here would contradict in-district precedent and the legal standards set by the Ninth Circuit.

Further, because of the nature of this allegation, the Court should apply the heightened pleading standard of Rule 9(b), since Plaintiffs' allegation is that Google misled users to profit off

[12] Plaintiffs' opposition also claims that Google sold GA for Firebase user data to third parties, citing FAC ¶¶ 200–04, but those paragraphs don't contain any such allegation.

[13] *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015) (Google's alleged cookie placement to track internet histories did not qualify for crime-tort exception, even if it constitutes intrusion upon seclusion); *Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. Mar. 28, 2001) (the crime-tort exception does not apply where the interceptor's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money"); *Cohen v. Casper Sleep Inc.*, No. 17-cv-9325, 2018 WL 3392877, at *4 (S.D.N.Y. July 12, 2018) (rejecting application of crime-tort exception because "collecting data to de-anonymize consumers was not Defendants' primary motivation" but "[r]ather … the means … to achieve their real purpose—marketing"); *In re Intuit Privacy Litig.*, 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001) (plaintiff alleged Intuit was "secretly tracking Class members' activities on the Internet . . . and profiting from the use of the illegally obtained information, all to Intuit's benefit.")

their private information. Yet, whether the heightened standard is applied or not, Plaintiffs do not come close to alleging a prima facie case for the crime-tort exception.

**III. Plaintiffs' CIPA claim fails.**

Mutual consent defeats this claim for the same reasons as the Wiretap Act claim. Plaintiffs' other arguments fail, too. First, CIPA applies to a person who "uses an electronic amplifying or recording device to eavesdrop," but Plaintiffs' allegations (other than their "secret scripts" theories) are that *app developers*, not Google, integrate Firebase SDK into their apps and *voluntarily enable* GA for Firebase. Google is, simply put, not the "person" who "uses" the "recording device." *See* Cal. Penal Code §§ 631(a), 632(a).

Second, Plaintiffs miss the point of Google's argument concerning "confidential" communications. Users were told by app developers that analytics services were being used to determine how their apps perform. Despite this, Plaintiffs claim they "reasonably expected that their communications were not being overheard, recorded, or otherwise being saved by Google (***or anyone***) when they took the affirmative step of turning off Web & App Activity." Opp. at 16. To give WAA the power Plaintiffs seek to give it is to ignore the reality of Plaintiffs' *factual* allegations. Their conclusions on this point are unreasonable.

Third, Plaintiffs attempt to distinguish case law holding that not all Internet communications give rise to an expectation of privacy. Plaintiffs assert that electronic communications can "in some circumstances" be confidential. Opp. 16; *cf. Revitch v. New Moosejaw, LLC*, No. 18-CV-06827-VC, 2019 WL 5485330, at *3 (N.D. Cal. Oct. 23, 2019). But they make no attempt to allege what particular internet communications are at issue here—or why they fall under that rubric.[14]

[14] The opposition claims Google has tried to rewrite the law by requiring an allegation that PII was collected, Opp. at 16:10–12, but Google never made such an argument. Google merely noted that *Plaintiffs* allege in conclusory fashion that their PII was collected, "but fail to identify what specific PII Google allegedly collected." Mot. at 16:1–6. As discussed, app developers are contractually barred from sending PII to Google via GA for Firebase.

## IV. Plaintiffs' constitutional and common law privacy claims fail.

In arguing they had a reasonable expectation of privacy, Plaintiffs misunderstand the lesson of *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 603 (9th Cir. 2020). The Ninth Circuit held that Facebook's "privacy disclosures . . . failed to acknowledge its tracking of logged-out users," and affirmatively told users that "[i]f you log out of Facebook, we will not receive this information about partner websites but you will also not see personalized experiences on these sites." *Id.* at 602. Here, in contrast, Google disclosed the collection of information through GA for Firebase, and never suggested that WAA could undo consent for GA for Firebase; to the contrary, Google affirmatively explained that consent for GA for Firebase is something to be taken up with individual apps and sites that use the service.

This case is thus indistinguishable from *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 954 (N.D. Cal. 2017), *aff'd*, 745 F. App'x 8 (9th Cir. 2018), where Facebook disclosed that it collected "information when you visit or use third-party websites and apps that use our Services." Although the "meaning of 'information' might be broad" and could include enough information to form a "browser fingerprint," this Court noted that "a contractual term is not ambiguous just because it is broad." The disclosures here are even more express—the app developers expressly agreed to obtain user consent. It would thus be objectively unreasonable to find an expectation of privacy.

Plaintiffs also argue that Google's conduct is "highly offensive" entirely on the basis of their "secret scripts" theory; they do not dispute that the consent for GA for Firebase eliminates any claim of a highly offensive invasion of privacy. Indeed, Plaintiffs do not respond to the raft of cases Google cited holding that, even where users allegedly *didn't* know about browsing history collection, it still did not rise to the "high bar" required to satisfy the "highly offensive" element.[15]

[15] *Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1047 (N.D. Cal. 2018) (Seeborg, J.), is distinguishable. There, Facebook was accused of "exploiting a vulnerability in prior versions of the Android OS permission settings" to overcome Google's security settings that protect user privacy where users had expressly asked Facebook not to collect exactly what it collected. *Id*. at 1047. Facebook didn't serve as a data servicer for a third party. And it made no effort to disclose its practices because they were, according to the allegations in that case, intended to be secret. Here, the secrecy allegations are undeserving of the presumption of truth, and the remaining allegations make clear that Google never hid what GA for Firebase does. Even if Plaintiffs are able to show that Google's efforts at obtaining consent were ineffective, that does not make what

**V. Plaintiffs' CDAFA claim fails.**

This claim is subject to the heightened pleading standard, too. *See Williams v. Facebook, Inc.*, 384 F. Supp. 3d 1043, 1053 (N.D. Cal. 2018). The entirety of Plaintiffs' argument that Google "acted without permission" in violation of CDAFA is based on their "secret scripts" theory. Without it, all that's left is mutual consent for GA for Firebase, a product that acts in accordance with its publicly-disclosed functionality.

As for the allegations relating to GA for Firebase, they cannot be characterized as lacking permission, much less overcoming technical barriers. *See id.* at 1053. Indeed, even if Google's efforts to obtain consent were ineffective, it still had permission from app developers in written contracts to do exactly what it did, and those developers were required to obtain consent too.

**VI. Plaintiffs' UCL claim fails for lack of standing, and for failure to state a claim.**

In defending their claim of UCL standing, Plaintiffs cobble together an argument that the UCL's long-standing "money or property" requirement has been altered by recently-enacted privacy laws. No case so holds. Their novel theory contradicts the long history of cases in this district and in California finding that claims like these lack UCL standing (see Mot. at 20–22, citing cases). Moreover, there is no evidence, including in the legislative history, that the laws Plaintiffs rely on were intended to overrule long-standing precedent.[16]

Plaintiffs' remaining argument has been tried and rejected in other cases. Plaintiffs never paid Google any money, and though they say now they gave apps money *solely because of Google' separate promises* related to WAA (which they unreasonably misconstrue), the FAC doesn't say that. *See* Opp. at 23 (citing FAC ¶ 313). At most, Plaintiffs had unreasonable subjective expectations about how their data would be treated, but the nine apps they've identified aren't paid apps, and it stretches credulity to think that any Plaintiff paid for Spanish lessons on the Duolingo app only because they believed Duolingo would use a company other than Google

---

happened here "highly offensive" and in violation of "community norms," a separate question subject to a separate, higher bar.

[16] Plaintiffs' reliance on *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 597 (9th Cir. 2020) is highly misleading. That case never addressed UCL standing; it discussed only Article III standing, which, as this Court well knows, is a broader concept.

for analytics, and had they known Google was providing the analytics service, then they would have sought a different language teacher. Certainly nothing in the FAC comes close to making such allegations. There isn't even an allegation of which apps Plaintiffs did pay money for. Plaintiffs attempt to cure this fatal flaw in their theory by alleging that "Google has used unlawful means to acquire money from a third party (the app developer) who had first obtained that money from Plaintiffs." But there is no allegation that Google acted to induce Plaintiffs to purchase any particular third-party app, so even Plaintiffs' cases wouldn't apply. And GA for Firebase is a tool app developers can use for free; charging for apps isn't a condition of its use. Apps charge for content, and that's what Plaintiffs received.[17]

As for the "unlawful" prong, none of Plaintiffs' claims can survive this motion to dismiss; they therefore cannot serve as the basis of a UCL claim. Plaintiffs do not dispute that the FTC Act, the FTC Settlement agreement with Google, and the CCPA are not predicate offenses. Additionally, Plaintiffs do not dispute that an alleged violation of the FTC consent order is not a cognizable predicate for an unlawful prong claim. Plaintiffs now claim instead that Google violated Cal. Bus. & Prof. Code § 22576 by violating its own Privacy Policy. That claim fails for the same reasons that doom their FAC: Google complied with its Privacy Policy.

Finally, Plaintiffs' single paragraph on the "unfair" prong doesn't respond to Google's motion. Once the "secret scripts" allegations are set aside, Plaintiffs fall far short of the standard.

**CONCLUSION**

For these reasons, Google respectfully requests that the Court dismiss Plaintiffs' First Amended Complaint in its entirety with prejudice.

[17] Plaintiffs cite to *In Re Anthem* to argue that money paid to app developers was eventually used to pay Google. Opp. at 23. *See In re Anthem, Inc. Data Breach Litig.*, No. 15-MD-02617-LHK, 2016 WL 3029783, at *30 (N.D. Cal. May 27, 2016). But here, Plaintiffs don't allege that they paid money to use the nine apps that are supported by Firebase SDK; and they don't make any allegation that this money was used to pay Google. And even assuming that Plaintiffs paid for the use of these nine apps, similar to *In re iPhone Application Litig*, Plaintiffs do not allege that they paid fees to Google and do not allege any facts establishing that the money paid to app developers was eventually used to pay Google. As such, Plaintiffs lack standing to bring their UCL claims.

WILLKIE FARR & GALLAGHER LLP

Date: February 4, 2021

By: */s/ Benedict Y. Hur*
BENEDICT Y. HUR
SIMONA AGNOLUCCI
EDUARDO E. SANTACANA
AMANDA MAYA

Attorneys for Defendant
Google LLC